FIG.1

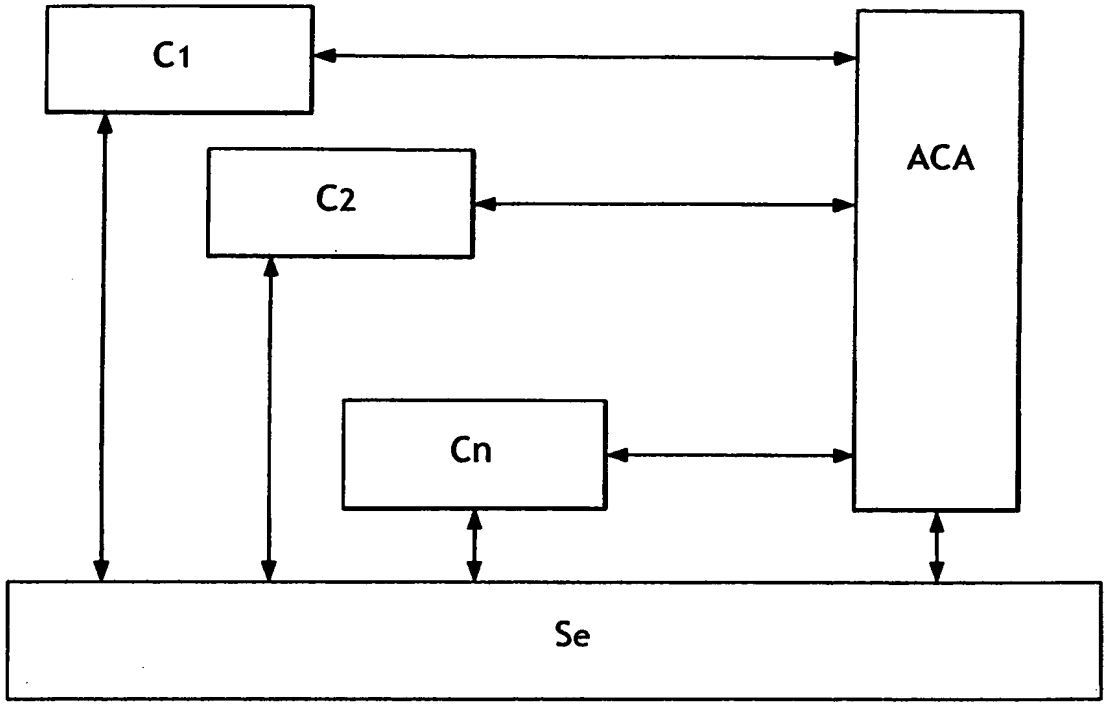
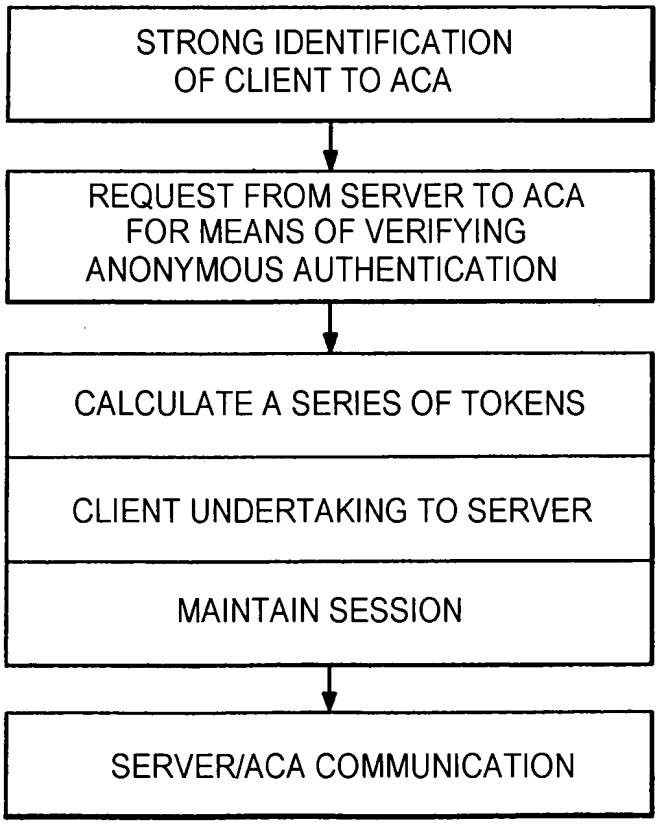

C1
C2
Cn
ACA
Se

FIG.2


STRONG IDENTIFICATION OF CLIENT TO ACA
REQUEST FROM SERVER TO ACA FOR MEANS OF VERIFYING ANONYMOUS AUTHENTICATION
CALCULATE A SERIES OF TOKENS
CLIENT UNDERTAKING TO SERVER
MAINTAIN SESSION
SERVER/ACA COMMUNICATION

10/534857
Rec'd PCT/PTO 13 MAY 2005

FIG.3

Initialization token-signing and session-opening protocol

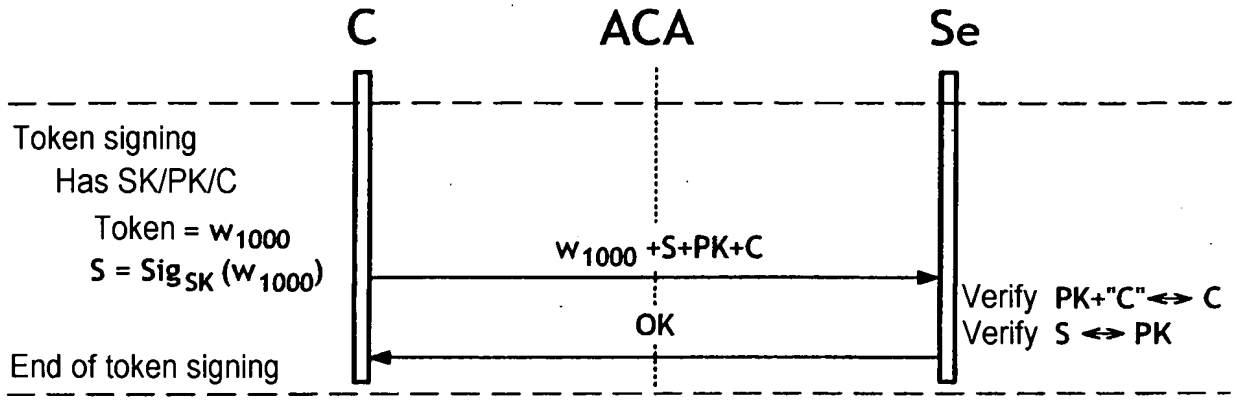


FIG.4

Anonymous certificate

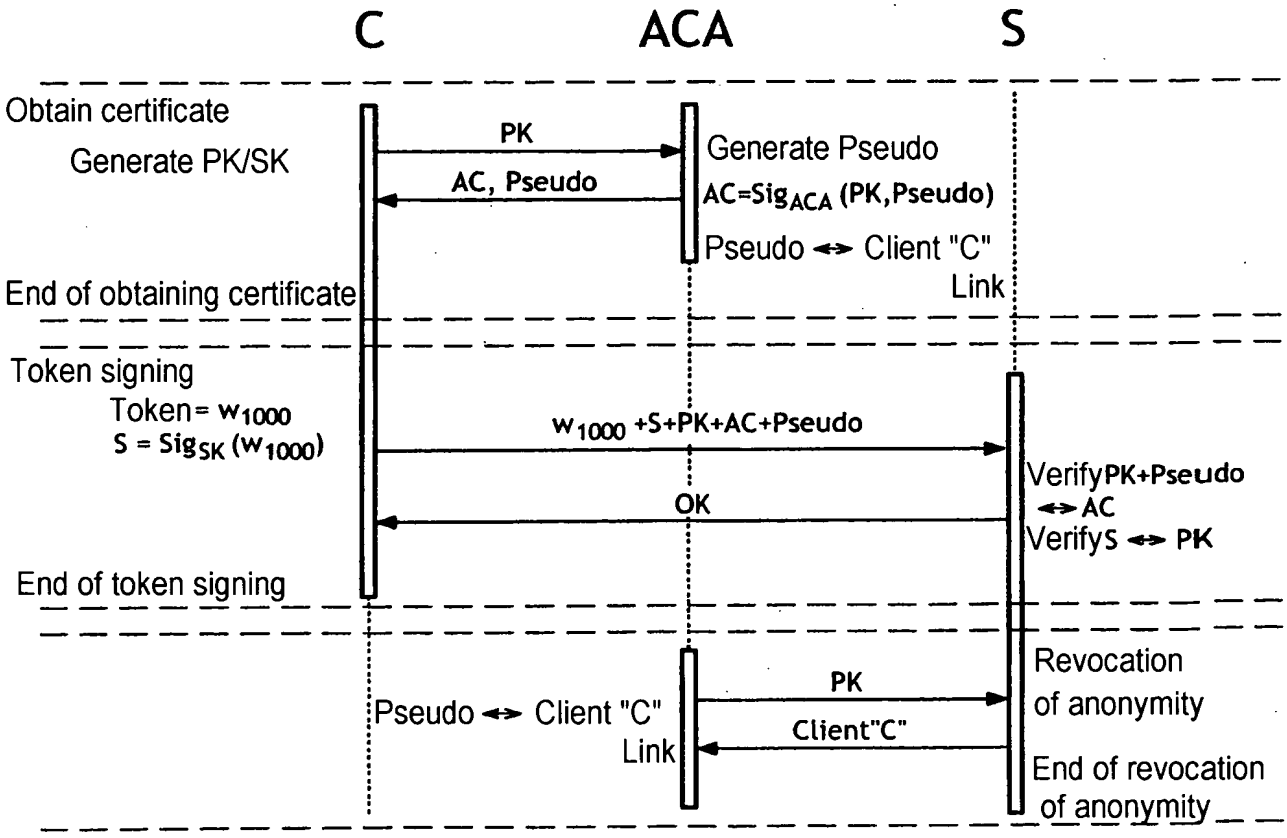


FIG.5

Blind signature with revocable anonymity

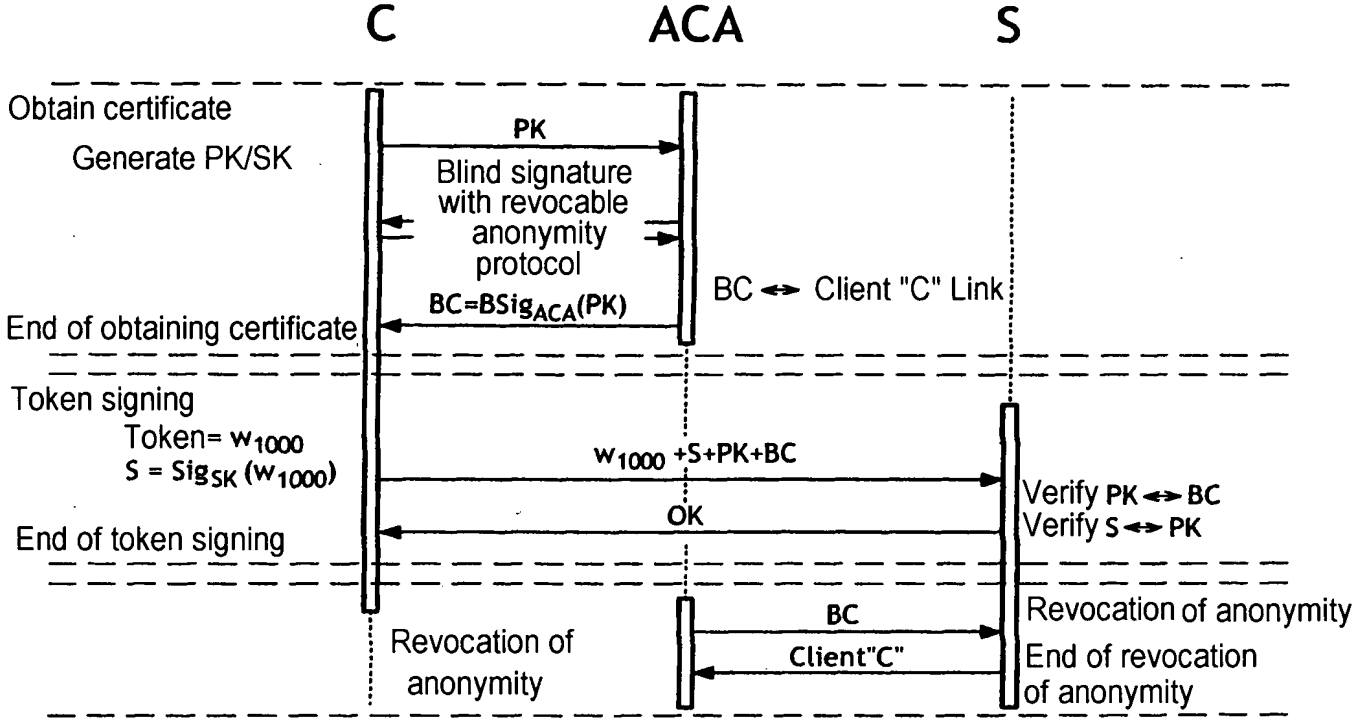


FIG.6

Group signature

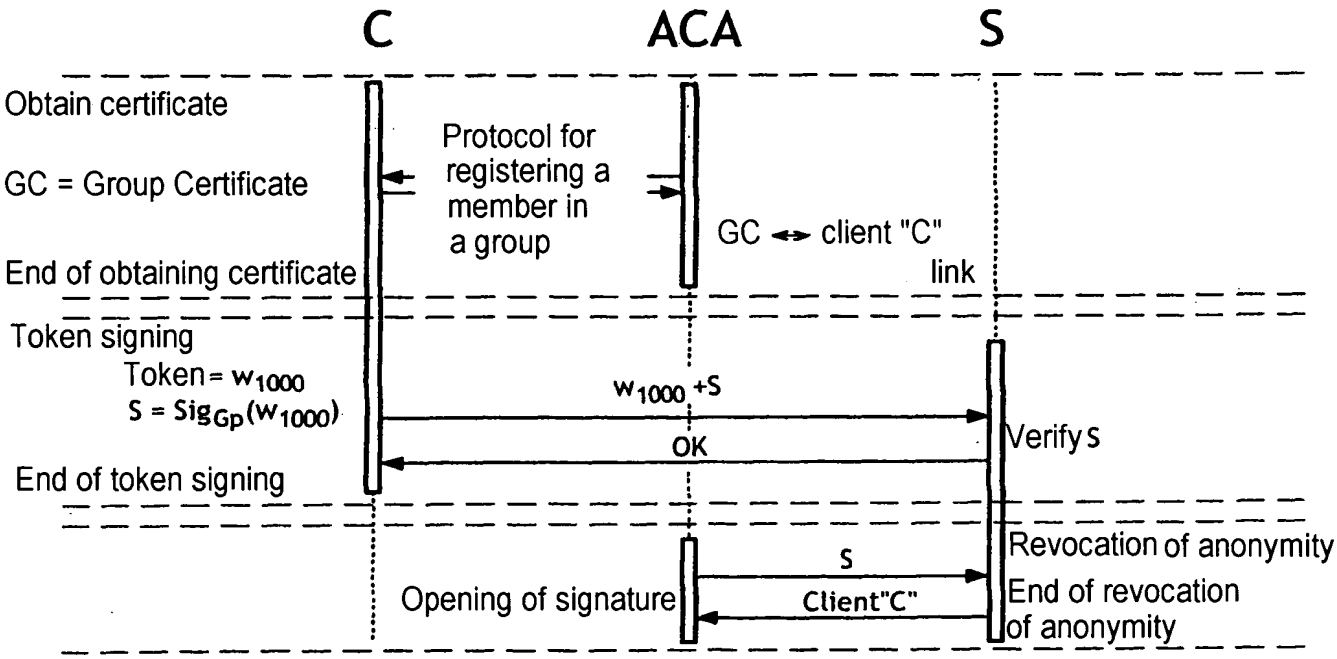


FIG.7

Server S: initialization				
Client C1		**Client C2**		Bid
Token	Value	Token	Value	Starting bid
W_{1000}	**signature**	X_{1000}	**signature**	**1000**

Instruction 1: Client 1 bid				
Client C1		**Client C2**		Bid
Token	Value	Token	Value	Current bid
W_{999}	***100***	X_{1000}	***0***	***1100***

Instruction 2: Client 1 bid				
Client C1		**Client C2**		Bid
Token	Value	Token	Value	Current bid
W_{999}	**100**	X_{997}	**3*100**	**1300**

Instruction 3: Client 1 bid				
Client C1		**Client C2**		Bid
Token	Value	Token	Value	Current bid
W_{996}	**4*100**	X_{997}	**3*100**	**1400**

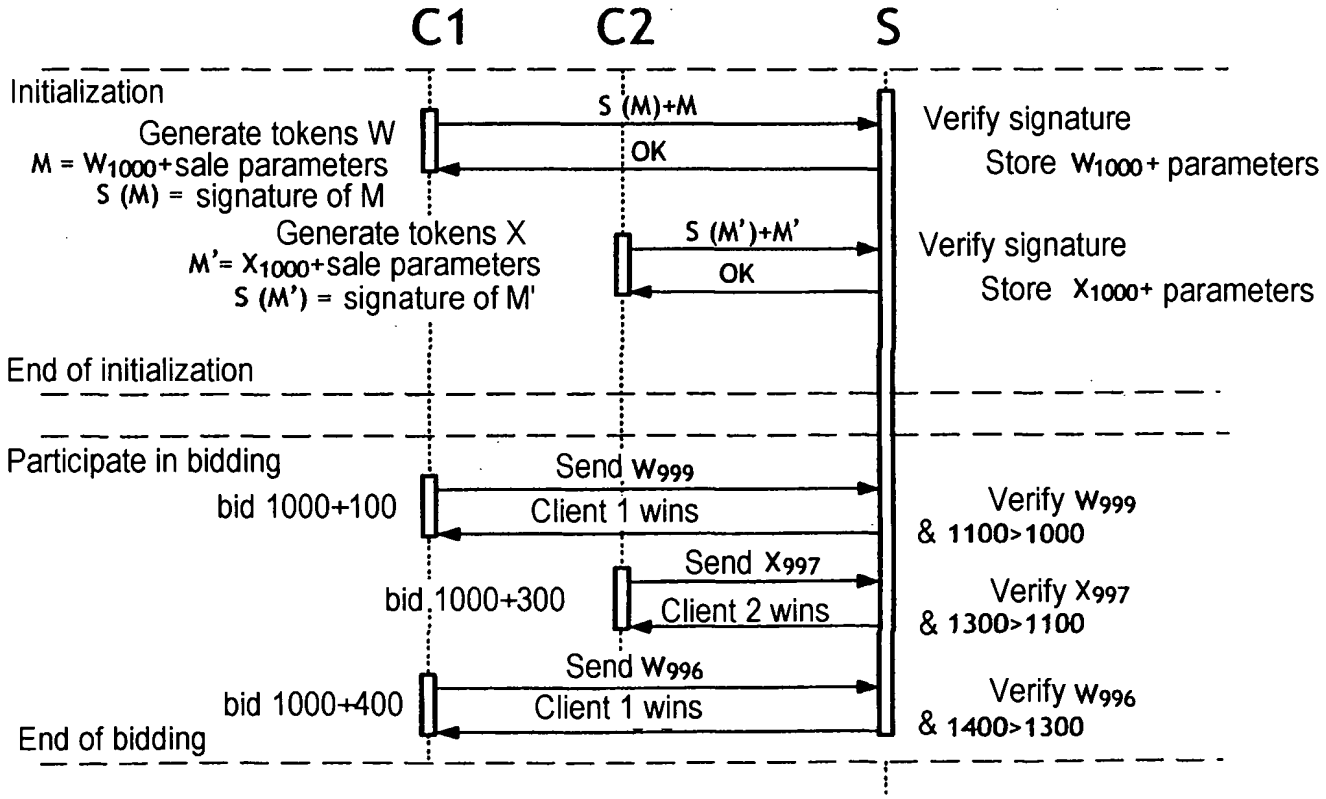


FIG.8

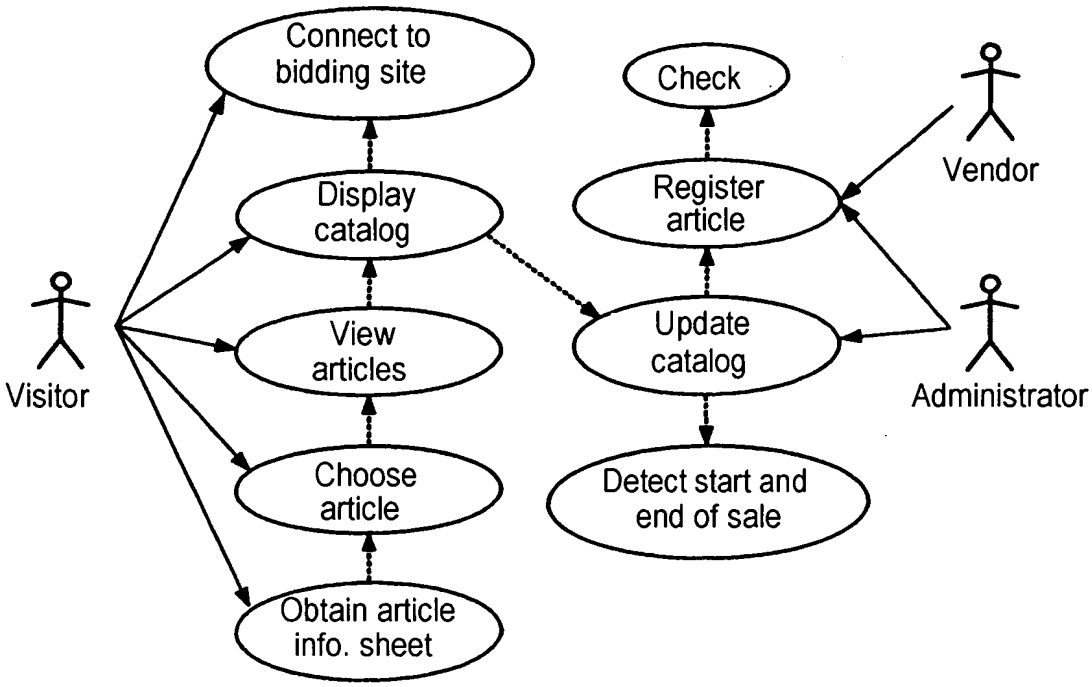

Connect to bidding site
Check
Vendor
Display catalog
Register article
View articles
Update catalog
Visitor
Administrator
Choose article
Detect start and end of sale
Obtain article info. sheet

FIG.9

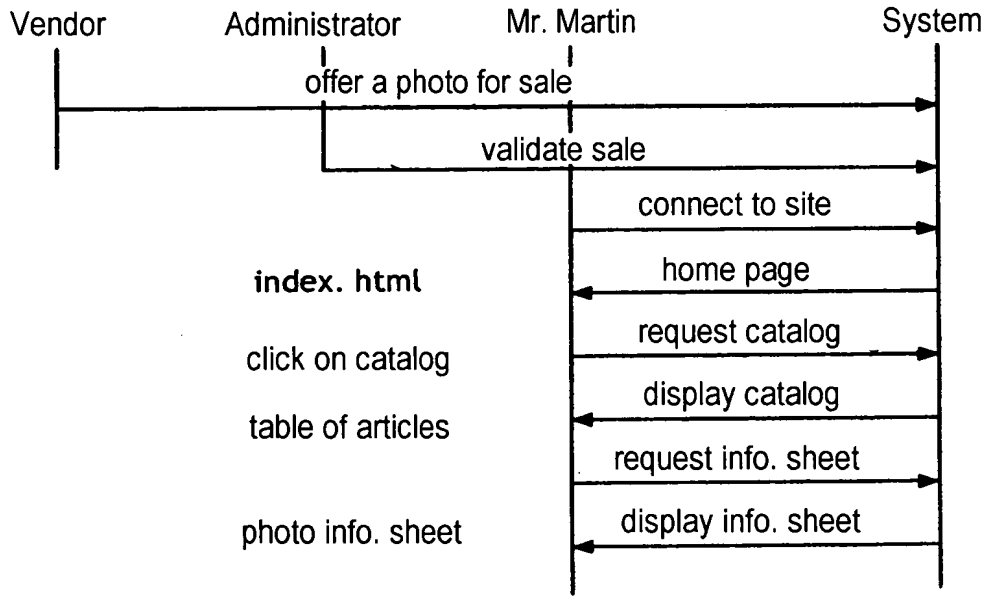

Vendor
Administrator
Mr. Martin
System
offer a photo for sale
validate sale
connect to site
index. html
home page
request catalog
click on catalog
display catalog
table of articles
request info. sheet
photo info. sheet
display info. sheet

FIG.10

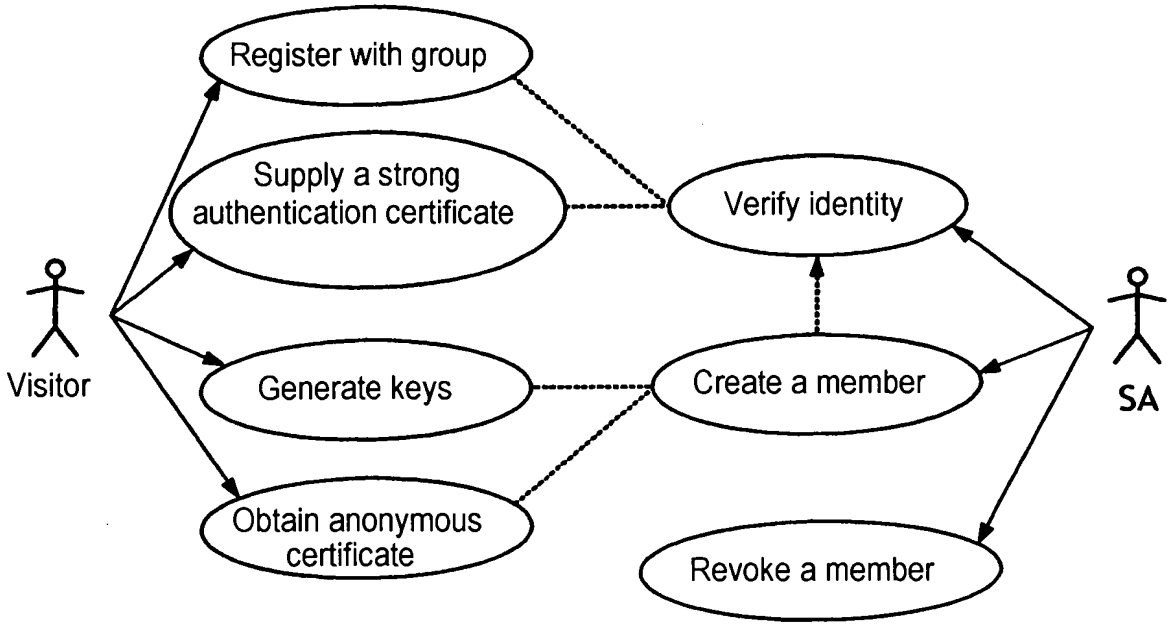

Register with group
Supply a strong authentication certificate
Verify identity
Visitor
Generate keys
Create a member
SA
Obtain anonymous certificate
Revoke a member

FIG.11

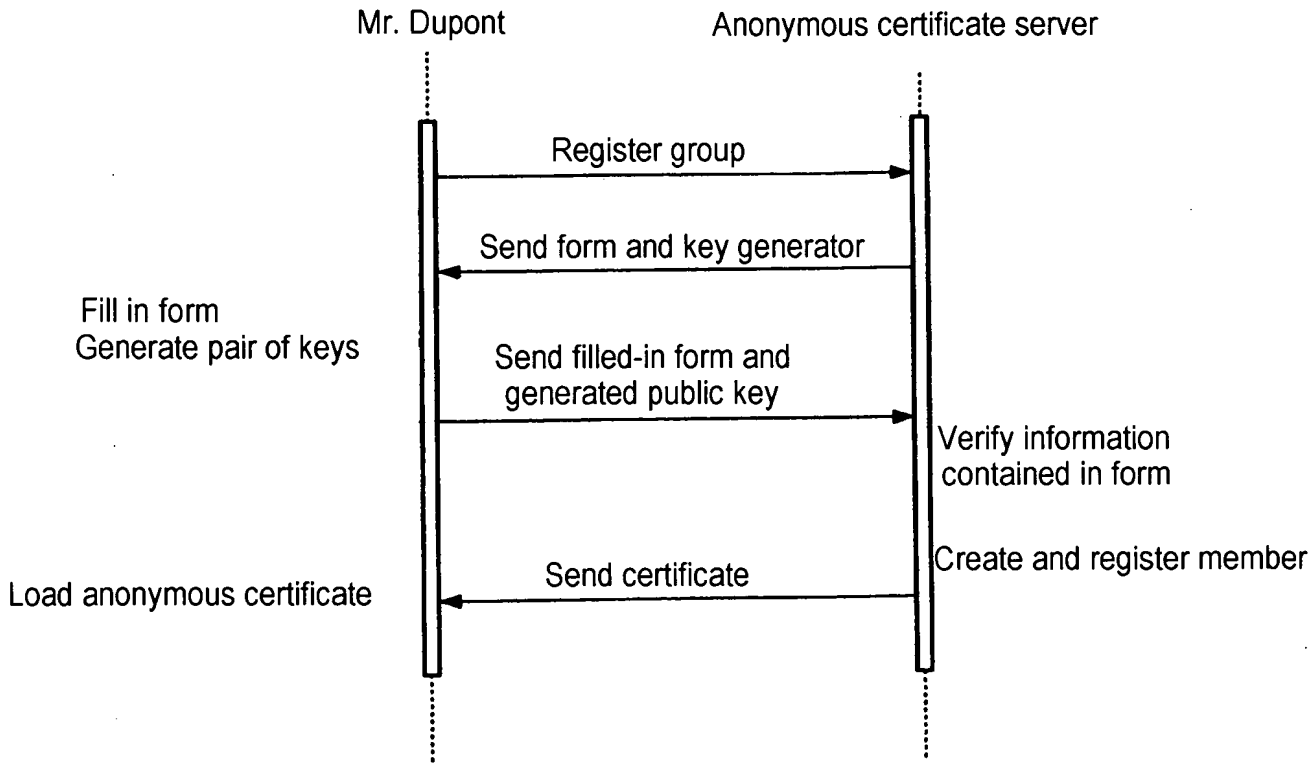

Mr. Dupont
Anonymous certificate server
Register group
Send form and key generator
Fill in form
Generate pair of keys
Send filled-in form and generated public key
Verify information contained in form
Create and register member
Send certificate
Load anonymous certificate

FIG.12

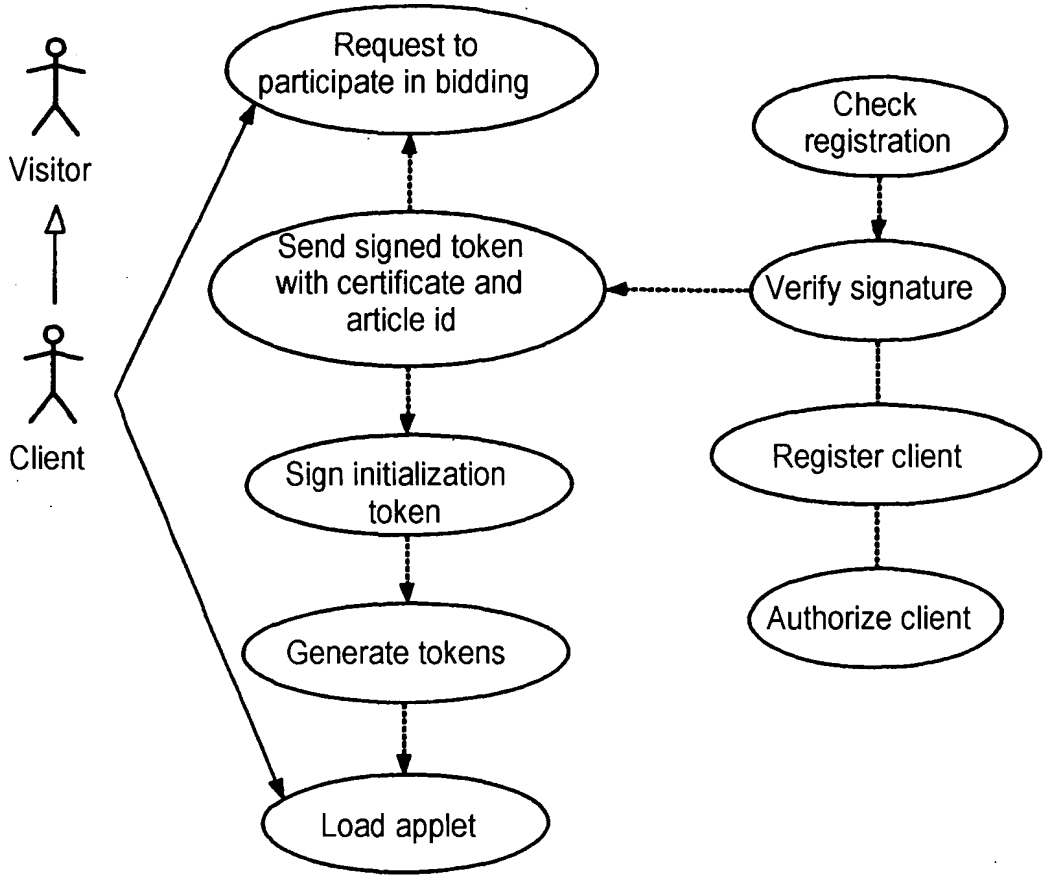

Visitor
Client
Request to participate in bidding
Send signed token with certificate and article id
Sign initialization token
Generate tokens
Load applet
Check registration
Verify signature
Register client
Authorize client

FIG.13

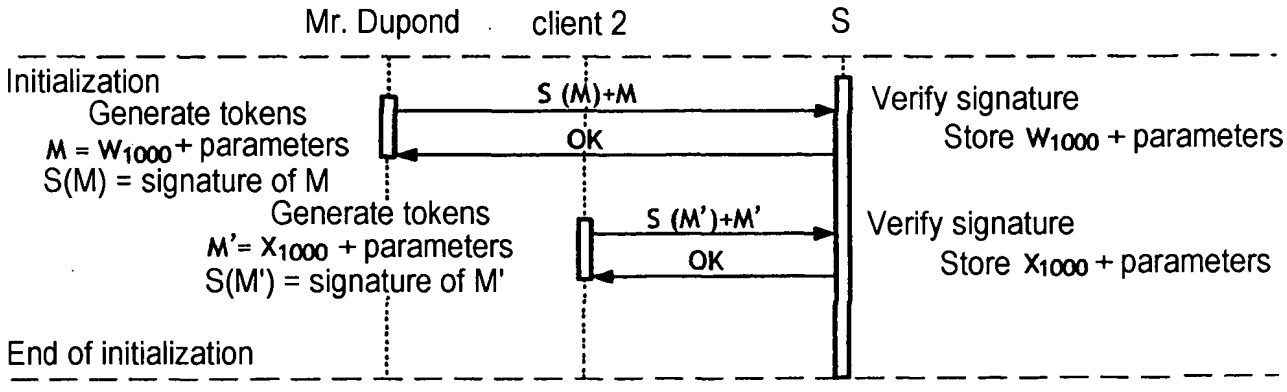

Mr. Dupond
client 2
S
Initialization
Generate tokens
M = W1000 + parameters
S(M) = signature of M
S (M)+M
OK
Verify signature
Store W1000 + parameters
Generate tokens
M'= X1000 + parameters
S(M') = signature of M'
S (M')+M'
OK
Verify signature
Store X1000 + parameters
End of initialization

FIG.14

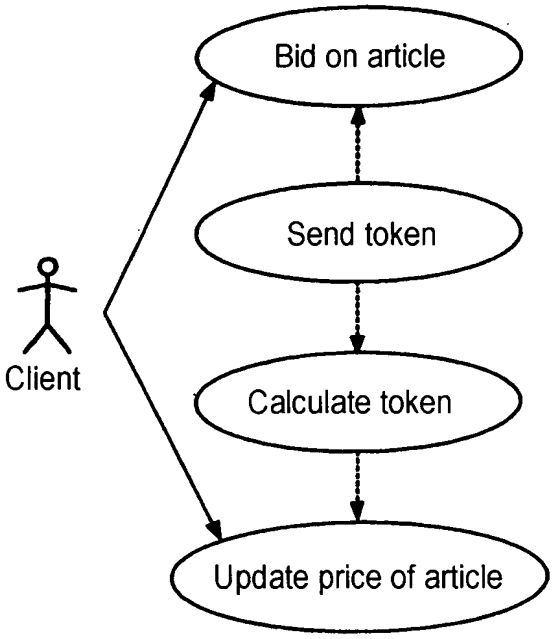

Bid on article
Send token
Client
Calculate token
Update price of article

FIG.15

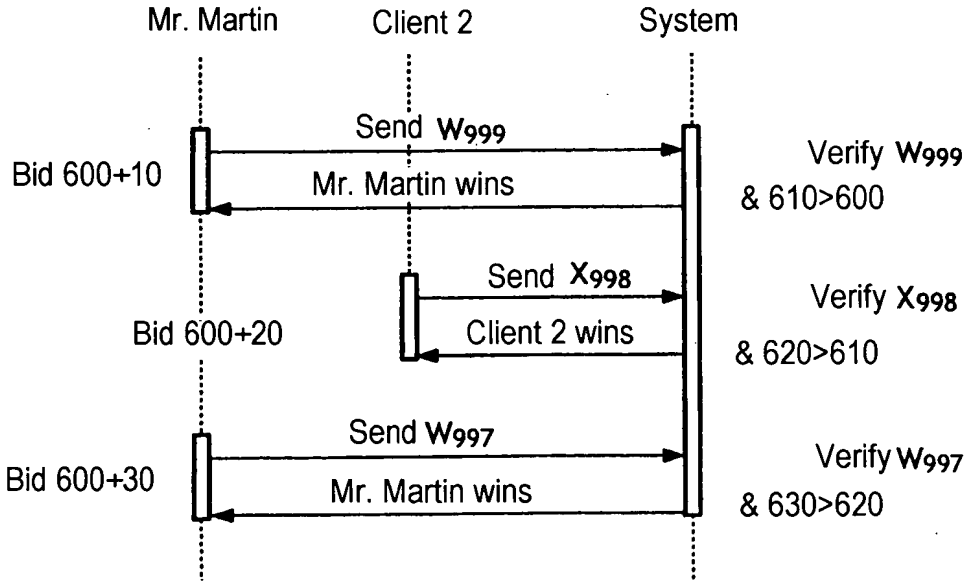

Mr. Martin
Client 2
System
Send W999
Bid 600+10
Mr. Martin wins
Verify W999
& 610>600
Send X998
Verify X998
Bid 600+20
Client 2 wins
& 620>610
Send W997
Verify W997
Bid 600+30
Mr. Martin wins
& 630>620

FIG.16

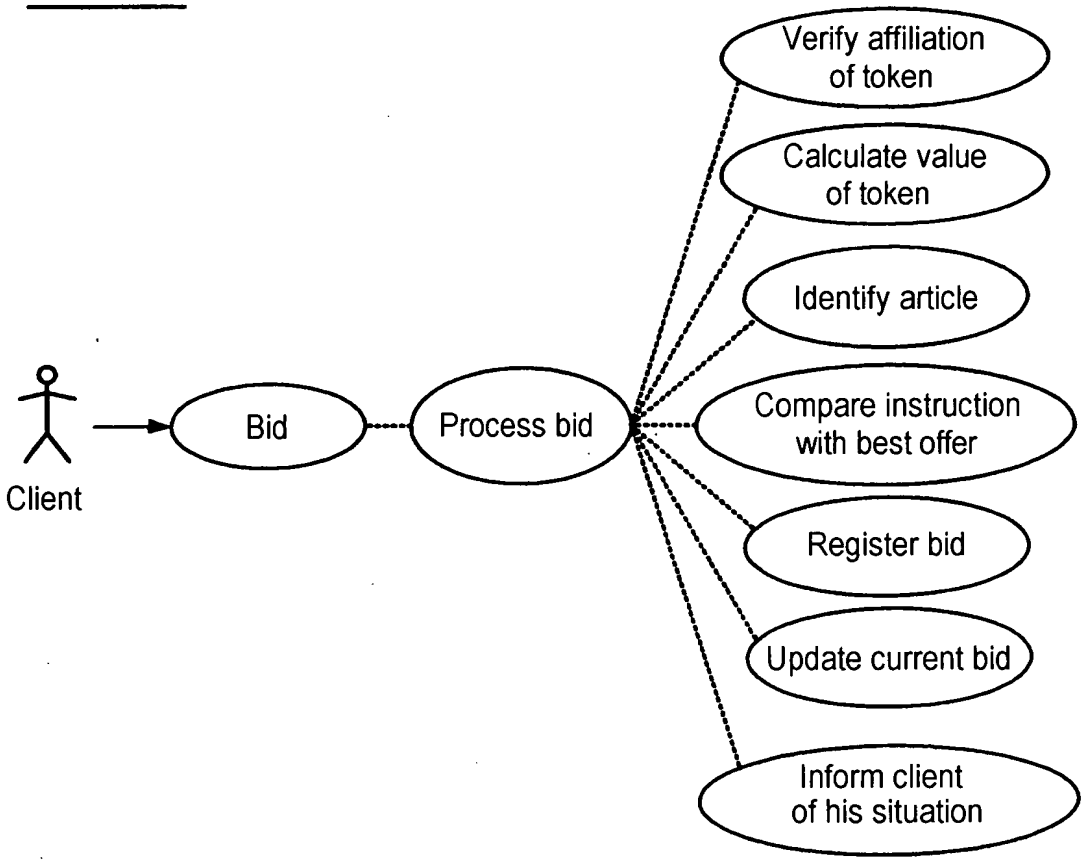

Verify affiliation of token
Calculate value of token
Identify article
Compare instruction with best offer
Register bid
Update current bid
Inform client of his situation
Bid
Process bid
Client

FIG.17

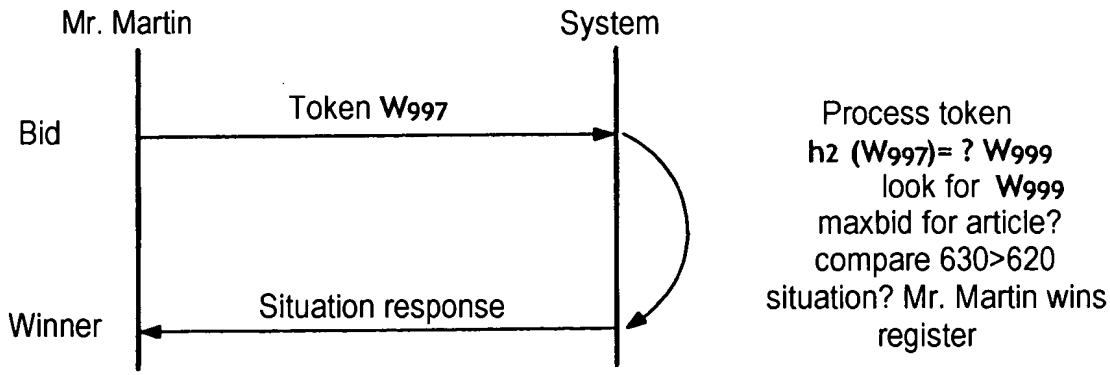

Mr. Martin
System
Bid
Token W997
Winner
Situation response
Process token
h2 (W997)= ? W999
look for W999
maxbid for article?
compare 630>620
situation? Mr. Martin wins
register

FIG.18

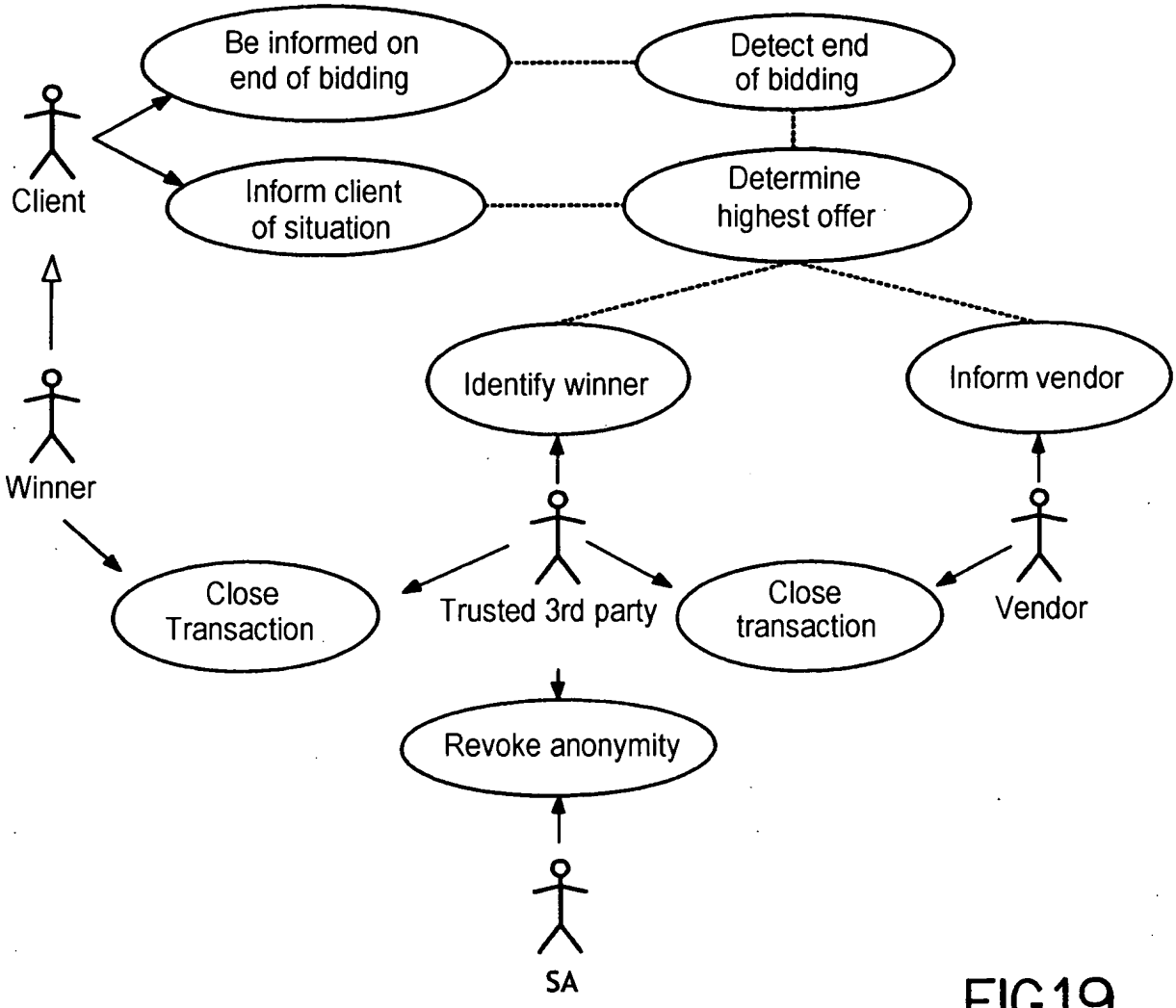

Be informed on end of bidding
Detect end of bidding
Client
Inform client of situation
Determine highest offer
Identify winner
Inform vendor
Winner
Close Transaction
Trusted 3rd party
Close transaction
Vendor
Revoke anonymity
SA

FIG.19

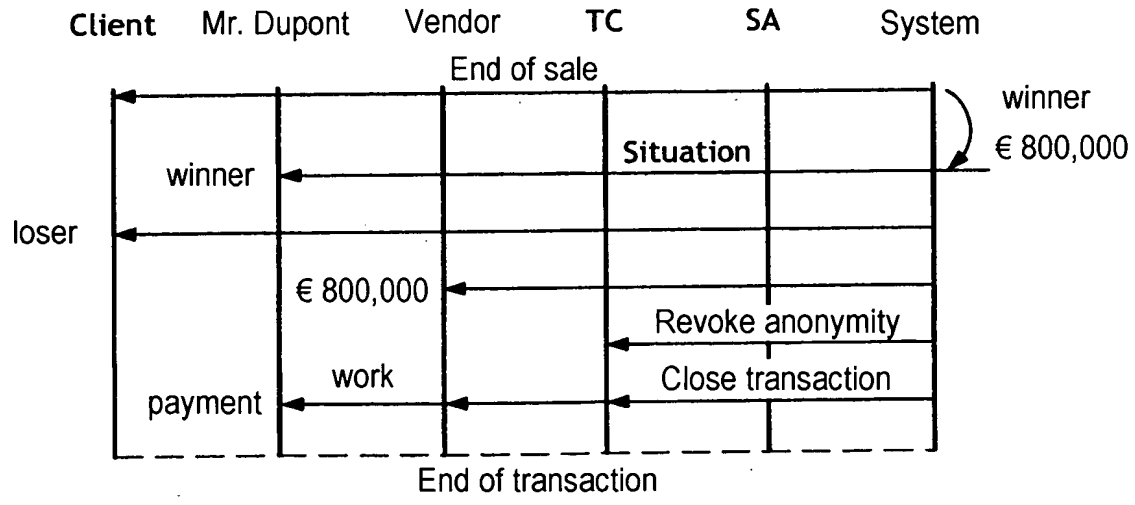
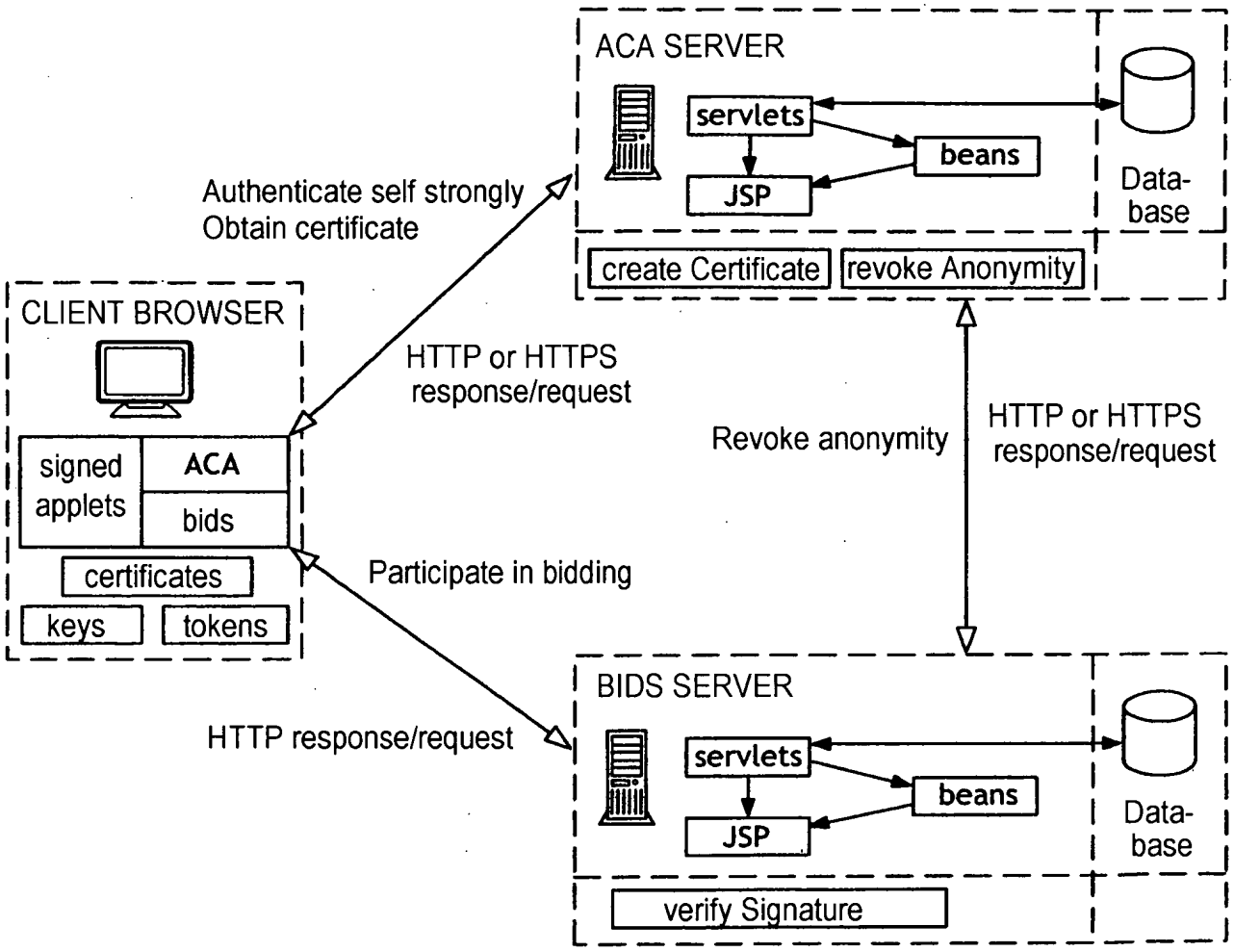

Client
Mr. Dupont
Vendor
TC
SA
System
End of sale
winner
€ 800,000
Situation
winner
loser
€ 800,000
Revoke anonymity
work
Close transaction
payment
End of transaction

FIG.20


ACA SERVER
servlets
beans
JSP
Data-
base
create Certificate
revoke Anonymity
Authenticate self strongly
Obtain certificate
CLIENT BROWSER
signed
applets
ACA
bids
certificates
keys
tokens
HTTP or HTTPS
response/request
Revoke anonymity
HTTP or HTTPS
response/request
Participate in bidding
HTTP response/request
BIDS SERVER
servlets
beans
JSP
Data-
base
verify Signature